ESET NOD32 Antivirus 4

pour Linux Desktop

Manuel d'installation et Guide de l'utilisateur

Cliquez ici pour télécharger la dernière version de ce document.



ESET NOD32 Antivirus 4

Service client Monde : www.eset.com/support

Rév. 8.4.2011

Sommaire

1. ESET NOD32 Antivirus

Conséquence de la popularité grandissante des systèmes d'exploitation Unix, les concepteurs de logiciels malveillants développent de plus en plus de menaces pour cibler les utilisateurs du système Linux. ESET NOD32 Antivirus propose une protection puissante et efficace contre les menaces. ESET NOD32 Antivirus permet de contrer les menaces Windows et protège les utilisateurs du système Linux lorsqu'ils interagissent avec les utilisateurs Windows. Les logiciels malveillants Windows ne constituent pas une menace directe pour Linux, mais la désactivation de logiciels malveillants qui ont infecté une machine Linux empêche sa propagation sur les ordinateurs Windows par l'intermédiaire d'un réseau local ou sur Internet.

1.1 Configuration système

La configuration système matérielle et logicielle minimale requise garantit le bon fonctionnement d'ESET NOD32 Antivirus :

ESET NOD32 Antivirus:

	Configuration système
Architecture du processeur	AMD®, Intel® 32 bits, 64 bits
Système	Distributions Debian et RedHat (Ubuntu, OpenSuse, Fedora, Mandriva, RedHat, etc.) kernel 2.6.x GNU C Library version 2.3 ou ultérieure GTK+ version 2.6 ou ultérieure Compatibilité LSB 3.1 recommandée
Mémoire	512 MB
Espace disponible	100 MB

2. Installation

Avant de commencer l'installation, fermez tous les programmes ouverts sur votre ordinateur. ESET NOD32 Antivirus contient des composants qui peuvent entrer en conflit avec les autres programmes antivirus qui sont peut-être installés sur votre ordinateur. ESET recommande vivement de supprimer tous les autres programmes afin d'éviter tout risque de problème. Vous pouvez installer ESET NOD32 Antivirus depuis un CD d'installation ou depuis un fichier disponible sur le site ESET.

Pour lancer l'assistant d'installation, effectuez l'une des opérations suivantes :

- Si vous effectuez l'installation depuis le CD d'installation, installez le CD dans le lecteur. Double-cliquez sur l'icône d'installation d'ESET NOD32 Antivirus pour lancer le programme d'installation.
- Si vous effectuez l'installation depuis un fichier téléchargé, cliquez avec le bouton droit sur le fichier, cliquez sur l'onglet **Propriétés > Autorisations**, cochez l'option d' **autorisation d'exécution du fichier en tant que programme** , puis fermez la fenêtre. Double-cliquez sur le fichier pour lancer le programme d'installation.

Lancez le programme d'installation ; l'Assistant Installation vous guidera dans les opérations de configuration de base. Après avoir accepté les termes du contrat de licence de l'utilisateur final, vous pouvez choisir les types d'installations suivants :

- Installation standard 5
- Installation personnalisée 5

2.1 Installation standard

L'installation standard comprend des options de configuration qui correspondent à la plupart des utilisateurs. Les paramètres offrent une sécurité maximale tout en permettant de conserver d'excellentes performances système. L'installation standard est l'option par défaut qui est recommandée si vous n'avez pas d'exigence particulière pour certains paramètres.

Le **système d'alerte anticipée ThreatSense.Net** contribue à garantir qu'ESET est informé immédiatement et en permanence des nouvelles infiltrations afin de protéger ses clients dans les meilleurs délais. Le système permet de soumettre les nouvelles menaces au laboratoire de recherche sur les menaces d'ESET, où elles sont analysées, traitées puis ajoutées à la base des signatures de virus. Par défaut, l'option **Activer le système d'alerte anticipée ThreatSense.Net** est sélectionnée. Cliquez sur **Configuration** pour modifier les paramètres détaillés de soumission des fichiers suspects. Pour plus d'informations, reportez-vous à la section ThreatSense.Net 19.

L'étape suivante de l'installation consiste à configurer la détection des applications potentiellement indésirables. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Bien que ces applications affichent habituellement une notification pendant l'installation, elles peuvent facilement s'installer sans votre consentement. Sélectionnez l'option **Activer la détection des applications potentiellement indésirables** pour autoriser ESET NOD32 Antivirus à détecter ce type de menace (recommandé). Si vous ne souhaitez pas activer cette fonctionnalité, sélectionnez l'option **Désactiver la détection des applications potentiellement indésirables**.

Cliquez sur **Installer** pour terminer l'installation.

2.2 Installation personnalisée

L'installation personnalisée est destinée aux utilisateurs expérimentés qui souhaitent modifier les paramètres avancés pendant l'installation.

Si vous utilisez un serveur proxy, vous pouvez définir ses paramètres maintenant en sélectionnant l'option **J'utilise un serveur proxy**. Entrez l'adresse IP ou l'adresse URL de votre serveur proxy dans le champ **Adresse**. Dans le champ **Port**, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut). Si le serveur proxy exige une authentification, saisissez un **nom d'utilisateur** et un **mot de passe** pour accorder l'accès au serveur proxy. Si vous êtes certain qu'aucun serveur proxy n'est utilisé, choisissez l'option **Je n'utilise pas de serveur proxy**.

Dans l'étape suivante, vous pouvez **définir les utilisateurs privilégiés** qui pourront modifier la configuration du programme. Dans la liste des utilisateurs figurant à gauche, sélectionnez les utilisateurs et l'option **Ajouter** pour les ajouter à la liste **Utilisateurs privilégiés**. Pour afficher tous les utilisateurs du système, sélectionnez l'option **Afficher tous les utilisateurs**.

Le **système d'alerte anticipée ThreatSense.Net** contribue à garantir qu'ESET est informé immédiatement et en permanence des nouvelles infiltrations afin de protéger ses clients dans les meilleurs délais. Le système permet de soumettre les nouvelles menaces au laboratoire de recherche sur les menaces d'ESET, où elles sont analysées, traitées puis ajoutées à la base des signatures de virus. Par défaut, l'option **Activer le système d'alerte anticipée ThreatSense.Net** est sélectionnée. Cliquez sur **Configuration** pour modifier les paramètres détaillés de soumission des fichiers suspects. Pour plus d'informations, reportez-vous à la section ThreatSense.Net 19.

L'étape suivante de l'installation consiste à configurer la détection des applications potentiellement indésirables. Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Bien que ces applications affichent habituellement une notification pendant l'installation, elles peuvent facilement s'installer sans votre consentement. Sélectionnez l'option **Activer la détection des applications potentiellement indésirables** pour autoriser ESET NOD32

Antivirus à détecter ce type de menace (recommandé).

Cliquez sur **Installer** pour terminer l'installation.

2.3 Activation de produit

Vous pouvez activer votre copie de ESET NOD32 Antivirus directement à partir du programme. Cliquez sur l'icône ESET NOD32 Antivirus située dans votre barre de menus (haut de l'écran), puis cliquez sur **Activation du produit...**

1. Si vous avez acheté une version du produit dans une boîte au détail, vous trouverez la clé d'activation avec les instructions détaillées d'activation. Cette clé d'activation se trouve généralement à l'intérieur ou au dos de l'emballage du produit. Vous devez entrer la clé d'activation exactement comme elle est indiquée.

2. Si vous avez reçu un nom d'utilisateur et un mot de passe, sélectionnez l'option **Activer à l'aide d'un nom d'utilisateur et d'un mot de passe**, puis entrez les données de licence dans les champs appropriés. Cette option est équivalente à **Configurer le nom d'utilisateur et le mot de passe...** dans la fenêtre Mise à jour du programme.

3. Si vous souhaitez évaluer ESET NOD32 Antivirus avant d'en faire l'acquisition, sélectionnez l'option **Activer la licence d'essai**. Indiquez votre nom et votre **Adresse électronique**. Votre licence de test sera envoyée à cette adresse. ESET NOD32 Antivirus sera activé pendant une période limitée. Les licences de test ne peuvent être activées qu'une seule fois par client.

Si vous n'avez pas de licence et souhaitez en acheter une, cliquez sur l'option **Acheter une licence**. Cette opération vous redirigera vers le site Web de votre distributeur ESET local.

2.4 Analyse de l'ordinateur à la demande

Après l'installation d'ESET NOD32 Antivirus, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse de l'ordinateur à la demande, reportez-vous à la section Analyse de l'ordinateur à la demande 10.

3. Guide du débutant

Ce chapitre donne un premier aperçu d'ESET NOD32 Antivirus et de ses paramètres de base.

3.1 Présentation de l'interface utilisateur : modes

La fenêtre principale d'ESET NOD32 Antivirus est divisée en deux sections principales. La fenêtre principale de droite affiche les informations correspondant à l'option sélectionnée dans le menu principal à gauche.

Voici une description des options disponibles dans le menu principal :

- **État de la protection** : fournit des informations sur l'état de protection d'ESET NOD32 Antivirus. Si l'option **Mode avancé** est activée, le sous-menu **Statistiques** apparaît.
- **Analyse de l'ordinateur** : cette option permet de configurer et de lancer l'**analyse de l'ordinateur à la demande**.
- **Mettre à jour** : affiche des informations sur les mises à jour de la base des signatures de virus.
- **Configuration** : sélectionnez cette option pour ajuster le niveau de sécurité de votre ordinateur. Si l'option **Mode avancé** est activée, le sous-menu **Antivirus et antispyware** apparaît.
- **Outils** : permet d'accéder aux fichiers journaux, aux **fichiers journaux**, à la **quarantaine** et au **planificateur**. Cette option n'apparaît qu'en **mode avancé**.
- **Aide** : fournit des informations sur le programme, et permet d'accéder aux fichiers d'aide, à la base de connaissances Internet et au site Internet d'ESET.

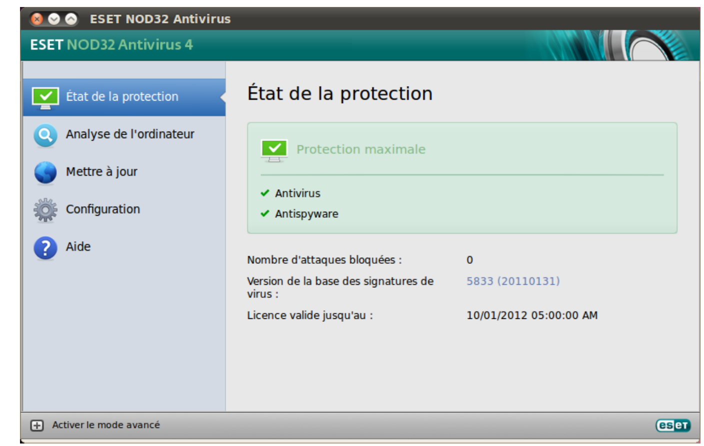
L'interface utilisateur d'ESET NOD32 Antivirus permet aux utilisateurs de passer du mode standard au mode avancé et inversement. Le mode standard permet d'accéder aux fonctionnalités nécessaires aux opérations classiques. Il n'affiche aucune option avancée. Pour passer d'un mode à l'autre, cliquez sur le signe plus (**+**) à côté de l'option **Activer le mode avancé/Activer le mode standard**, dans l'angle inférieur gauche de la fenêtre principale du programme.

Le mode Standard donne accès aux fonctionnalités nécessaires aux opérations ordinaires. Il n'affiche aucune option avancée.

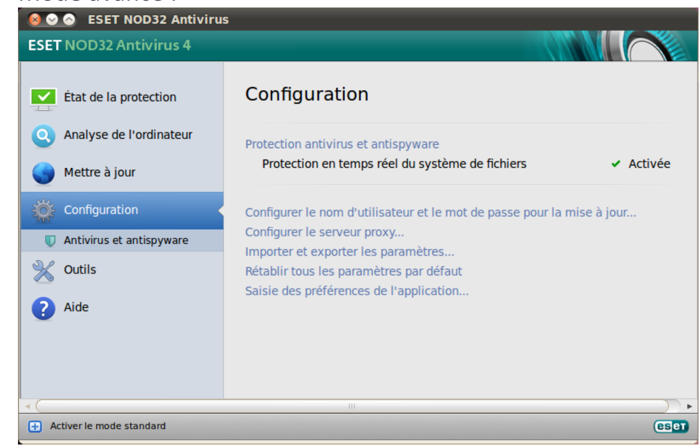
Le passage au mode avancé ajoute l'option **Outils** dans le menu principal. L'option **Outils** permet d'accéder à des sous-menus concernant les **fichiers journaux**, la **quarantaine** et le **planificateur**.

REMARQUE : toutes les instructions de ce guide sont effectuées en **mode avancé**.

Mode standard :

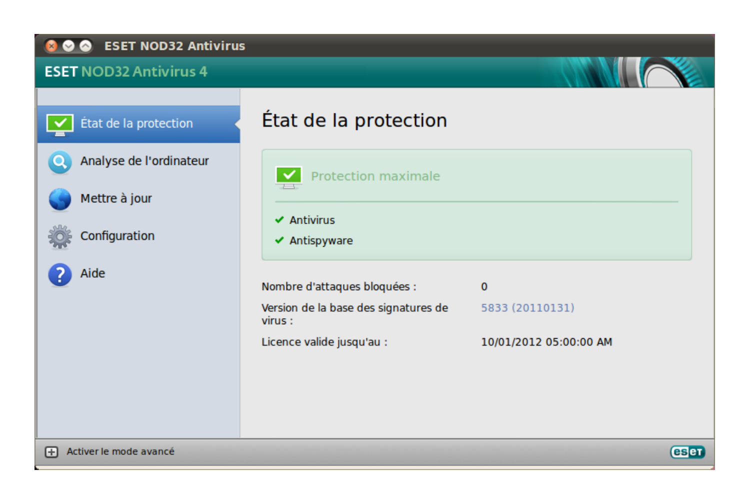


Mode avancé :



3.1.1 Contrôle du fonctionnement du système

Pour afficher l'**état de la protection**, cliquez sur l'option en haut du menu principal. La fenêtre principale affiche un résumé de l'état de fonctionnement d'ESET NOD32 Antivirus et un sous-menu concernant des **statistiques**. Sélectionnez cette option pour afficher des informations détaillées et des statistiques concernant les analyses de l'ordinateur qui ont été réalisées sur votre système. La fenêtre Statistiques est disponible uniquement en mode avancé.



3.1.2 Que faire lorsque le programme ne fonctionne pas correctement ?

Une icône verte s'affiche en regard de chaque module activé et fonctionnant correctement. Dans le cas contraire, un point d'exclamation rouge ou orange et des informations supplémentaires sur le module s'affichent dans la partie supérieure de la fenêtre. Une suggestion de solution pour corriger le module est également affichée. Pour changer l'état des différents modules, cliquez sur **Configuration** dans le menu principal puis sur le module souhaité.

Si vous ne parvenez pas à résoudre le problème à l'aide des solutions suggérées, cliquez sur **Aide** pour accéder aux fichiers d'aide ou pour effectuer des recherches dans la base de connaissances.

Si vous avez besoin d'aide, vous pouvez contacter le service client d'ESET sur le site Internet d'ESET. Le service client d'ESET répondra très rapidement à vos questions et vous permettra de déterminer une solution.



4. Utiliser ESET NOD32 Antivirus

4.1 Protection antivirus et antispyware

La protection antivirus protège des attaques contre le système en modifiant les fichiers représentant des menaces potentielles. Si une menace comportant du code malveillant est détectée, le module Antivirus peut l'éliminer en la bloquant. Il peut ensuite la nettoyer, la supprimer ou la placer en quarantaine.

4.1.1 Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers contrôle tous les événements liés à l'antivirus dans le système. Lorsque ces fichiers sont ouverts, créés ou exécutés sur l'ordinateur, elle les analyse pour y rechercher la présence éventuelle de code malveillant. La protection en temps réel du système de fichiers est lancée au démarrage du système.

4.1.1.1 Configuration de la protection en temps réel

La protection en temps réel du système de fichiers vérifie tous les types de supports et l'analyse est déclenchée par différents événements. L'utilisation des méthodes de détection de la technologie ThreatSense (décrites dans la section intitulée Configuration des paramètres du moteur ThreatSense 12), la protection du système de fichiers en temps réel est différente pour les nouveaux fichiers et pour les fichiers existants. Pour les nouveaux fichiers, il est possible d'appliquer un niveau de contrôle plus approfondi.

Par défaut, la protection en temps réel est lancée au démarrage du système d'exploitation, assurant ainsi une analyse ininterrompue. Dans certains cas (par exemple, en cas de conflit avec un autre analyseur en temps réel), il est possible de mettre fin à la protection en temps réel en cliquant sur l'icône ESET NOD32 Antivirus dans la barre de menus (en haut de l'écran), puis en sélectionnant l'option **Désactiver la protection en temps réel du système de fichiers** . Il est également possible de mettre fin à la protection en temps réel depuis la fenêtre principale du programme (**Configuration** > **Antivirus et antispyware** > **Désactiver**).

Pour modifier les paramètres avancés de la protection en temps réel, sélectionnez **Configuration** > **Saisie des préférences de l'application...** > **Protection** > **Protection en temps réel** et cliquez sur le bouton **Configuration...** situé à côté de **Options avancées** (reportez-vous à la section Options d'analyse avancées 9).

4.1.1.1.1 Analyser le (analyse déclenchée par un événement)

Par défaut, tous les fichiers sont analysés à l'**ouverture**, à la **création** ou à l'**exécution**. Il est recommandé de conserver les paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur.

4.1.1.1.2 Options d'analyse avancées

Vous pouvez définir dans cette fenêtre les types d'objet que le moteur ThreatSense doit analyser, activer/désactiver l'option **Heuristique avancée** et modifier les paramètres des archives et du cache de fichiers.

Il n'est pas recommandé de modifier les valeurs par défaut de la section **Paramètres d'archive par défaut**, à moins que vous n'ayez besoin de résoudre un problème spécifique, car l'augmentation des valeurs d'imbrication des archives peut avoir une incidence sur les performances.

Vous pouvez activer ou désactiver l'analyse heuristique avancée ThreatSense de chacun des fichiers exécutés, créés et modifiés en sélectionnant ou en désélectionnant la case **Heuristique avancée** de chaque section de paramètres ThreatSense.

Pour réduire l'impact de la protection en temps réel sur le système, vous pouvez définir la taille du cache d'optimisation. Ce comportement est actif lorsque vous utilisez l'option **Activer le cache des fichiers nettoyés**. Si cette fonction est désactivée, tous les fichiers sont analysés à chaque accès. Les fichiers ne sont analysés qu'une seule fois après leur mise en cache (sauf s'ils ont été modifiés), jusqu'à ce que la taille définie pour le cache soit atteinte. Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base des signatures de virus.

Cliquez sur **Activer le cache des fichiers nettoyés** pour activer/désactiver cette fonction. Pour définir la quantité de fichiers à mettre en cache, il vous suffit d'entrer la valeur souhaitée dans le champ de saisie situé à côté de l'option **Taille du cache** .

D'autres paramètres d'analyse peuvent être définis dans la fenêtre **Configuration du moteur ThreatSense**. Vous pouvez définir le type des **objets** à analyser, les **options** à utiliser et le niveau de **nettoyage**, les **extensions** et les **limites** de taille de fichiers pour la protection du système de fichiers en temps réel. Vous pouvez ouvrir la fenêtre de configuration du moteur ThreatSense en cliquant sur le bouton **Configuration** situé à côté de l'option **Moteur ThreatSense** dans la fenêtre Configuration avancée. Pour plus d'informations sur les paramètres du moteur ThreatSense, reportez-vous à la section Configuration des paramètres du moteur ThreatSense 12.

4.1.1.1.3 Exclusions de l'analyse

Cette section permet d'exclure certains fichiers et dossiers de l'analyse.

- **Chemin** : chemin d'accès aux fichiers et dossiers exclus.
- **Menace** : si le nom d'une menace figure à côté d'un fichier exclu, cela signifie que ce fichier n'est exclu que pour cette menace spécifique : il n'est pas exclu complètement. Par conséquent, si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté par le module antivirus.

- **Ajouter** : exclut les objets de la détection. Saisissez le chemin d'accès à l'objet (vous pouvez également utiliser les caractères génériques * et ?) ou sélectionnez le dossier ou le fichier dans l'arborescence.
- **Modifier** : permet de modifier des entrées sélectionnées.
- **Supprimer** : supprime les entrées sélectionnées.
- **Par défaut** : annule toutes les exclusions.

4.1.1.2 Quand faut-il modifier la configuration de la protection en temps réel ?

La protection en temps réel est le composant essentiel de la sécurisation du système. Procédez avec prudence lorsque vous modifiez les paramètres de protection en temps réel. Il est recommandé de ne modifier ces paramètres que dans des cas très précis. Vous pouvez les modifier par exemple lorsqu'il y a conflit avec une autre application ou avec l'analyseur en temps réel d'un autre logiciel antivirus.

Après l'installation d'ESET NOD32 Antivirus, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Afin de restaurer les paramètres par défaut, cliquez sur le bouton **Par défaut** situé dans la partie inférieure gauche de la fenêtre **Protection en temps réel** (**Configuration** > **Saisie des préférences de l'application...** > **Protection** > **Protection en temps réel**).

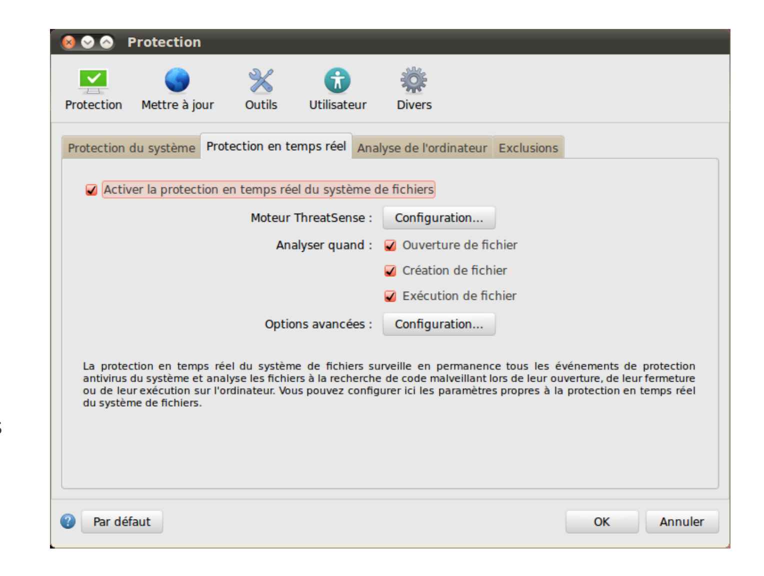
4.1.1.3 Vérification de la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne correctement et qu'elle détecte les virus, utilisez le fichier de test eicar.com. Ce fichier de test est un fichier inoffensif particulier qui est détectable par tous les programmes antivirus. Le fichier a été créé par l'institut EICAR (European Institute for Computer Antivirus Research) pour tester la fonctionnalité des programmes antivirus.

4.1.1.4 Que faire si la protection en temps réel ne fonctionne pas ?

Dans ce chapitre, nous décrivons des problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel et la façon de les résoudre.

La protection en temps réel est désactivée
Si la protection en temps réel a été désactivée par inadvertance par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, sélectionnez **Configuration** > **Antivirus et antispyware** et cliquez sur le lien **Activer la protection en temps réel du système de fichiers** (à droite) dans la fenêtre principale du programme. Vous pouvez également activer la protection du système de fichiers en temps réel dans la fenêtre Configuration avancée : sélectionnez **Protection** > **Protection en temps réel** et **Activer la protection en temps réel du système de fichiers**.



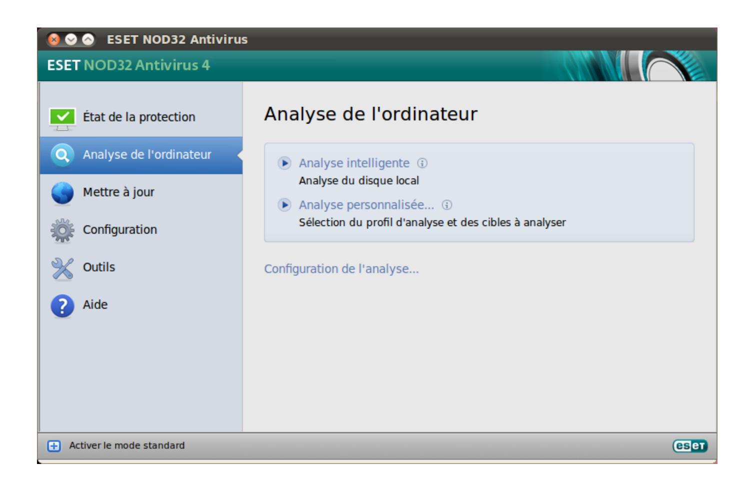
La protection en temps réel ne détecte et ne nettoie pas les infiltrations
Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Il est recommandé de désinstaller tout autre antivirus de votre système.

La protection en temps réel ne démarre pas
Si la protection en temps réel n'est pas initialisée au démarrage du système, cela peut provenir de conflits avec d'autres programmes. Dans ce cas, consultez les spécialistes du service client ESET.

4.1.2 Analyse de l'ordinateur à la demande

Si vous pensez que votre ordinateur peut être infecté (en raison d'un comportement anormal), exécutez **Analyse de l'ordinateur** > **Analyse intelligente** pour rechercher d'éventuelles infiltrations. Pour une protection maximum, les analyses d'ordinateur doivent être exécutées régulièrement dans le cadre de mesures de sécurité de routine. Elles ne doivent pas être exécutées uniquement lorsqu'une infection est suspectée. Une analyse régulière peut détecter des infiltrations n'ont détectées par l'analyseur en temps réel au moment de leur enregistrement sur le disque. Cela peut se produire si l'analyseur en temps réel est désactivé au moment de l'infection ou si la base des signatures de virus n'est plus à jour.

Nous recommandons d'exécuter une analyse d'ordinateur à la demande au moins une fois par mois. L'analyse peut être configurée comme tâche planifiée dans **Outils** > **Planificateur**.



4.1.2.1 Type d'analyse

Deux types d'analyses de l'ordinateur à la demande sont disponibles. L'**analyse intelligente** analyse le système sans exiger de reconfiguration des paramètres d'analyse. L'**analyse personnalisée** permet de sélectionner l'un des profils d'analyse prédéfinis, ainsi que de choisir des cibles spécifiques à analyser.

4.1.2.1.1 Analyse intelligente

L'analyse intelligente permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. Elle présente l'avantage d'être facile à utiliser, sans aucune configuration d'analyse détaillée. L'analyse intelligente vérifie tous les fichiers de tous les dossiers, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage 13.

4.1.2.1.2 Analyse personnalisée

L'**Analyse personnalisée** est la solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. L'analyse personnalisée présente l'avantage de permettre de configurer les paramètres avec grande précision. Les configurations peuvent être enregistrées sous forme de profils d'analyse définis par l'utilisateur, utiles pour effectuer régulièrement une analyse avec les mêmes paramètres.

Pour sélectionner des cibles à analyser, sélectionnez **Analyse de l'ordinateur** > **Analyse personnalisée**, puis des **cibles à analyser** spécifiques dans l'arborescence. Une cible d'analyse peut aussi être spécifiée plus précisément : vous devez indiquer le chemin d'accès au dossier ou aux fichiers à inclure. Si vous souhaitez uniquement effectuer une analyse du système sans ajouter d'actions de nettoyage supplémentaires, sélectionnez l'option **Analyse sans nettoyage**. Vous pouvez aussi choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration...** > **Nettoyage**.

L'exécution d'analyses personnalisées de l'ordinateur est recommandée pour les utilisateurs chevronnés qui maîtrisent l'utilisation de programmes antivirus.

4.1.2.2 Cibles à analyser

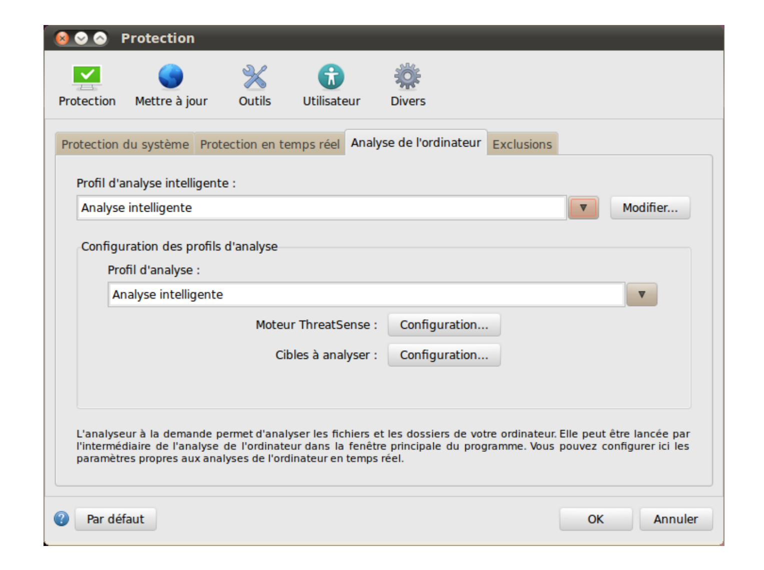
L'arborescence des cibles à analyser permet de sélectionner les fichiers et dossiers à soumettre à l'analyse antivirus. Les dossiers peuvent également être sélectionnés, en fonction aux paramètres d'un profil.

Une cible d'analyse peut aussi être définie plus précisément en entrant le chemin du dossier ou des fichiers à inclure dans l'analyse. Sélectionnez les cibles dans l'arborescence des dossiers disponibles sur l'ordinateur.

4.1.2.3 Profils d'analyse

Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un profil, sélectionnez **Configuration** > **Saisie des préférences de l'application...** > **Protection** > **Analyse de l'ordinateur** et cliquez sur l'option **Modifier** à côté de la liste des profils en cours.



Pour plus d'informations sur la création d'un profil d'analyse, reportez-vous à la section Configuration du moteur ThreatSense 12 ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

Exemple : Supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse, la configuration d'analyse intelligente est partiellement adéquate, mais vous ne souhaitez analyser ni les fichiers exécutables compressés par un compresseur d'exécutables, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un nettoyage strict. Dans la fenêtre **Liste des profils de l'analyseur à la demande**, saisissez le nom du profil, cliquez sur le bouton **Ajouter** et confirmez en cliquant sur **OK**. Réglez ensuite les paramètres pour qu'ils correspondent à vos besoins en configuration les options **Moteur ThreatSense** et **Cibles à analyser**.



4.1.3 Configuration du moteur ThreatSense

ThreatSense est une technologie qui comprend des méthodes de détection de menaces complexes. C'est une technologie proactive : elle fournit également une protection dès les premières heures de propagation d'une nouvelle menace. Elle utilise une combinaison de plusieurs méthodes (analyse de code, émulation de code, signatures génériques, signatures de virus) qui se conjuguent pour améliorer sensiblement la sécurité du système. Ce moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, ce qui maximise l'efficacité et le taux de détection. La technologie ThreatSense élimine avec succès les rootkits.

Les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :
- les types de fichiers et les extensions à analyser ;
- la combinaison de plusieurs méthodes de détection ;
- les niveaux de nettoyage, etc.

Pour accéder à la fenêtre de configuration, cliquez sur **Configuration** > **Antivirus et antispyware** > **Configuration avancée de la protection antivirus et anti-logiciels espions**, puis sur le bouton **Configuration** situé dans les zones **Protection du système**, **Protection en temps réel** et **Analyse de l'ordinateur** qui utilisent tous la technologie ThreatSense (voir ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. ThreatSense est configurable individuellement pour les modules de protection suivants :
- **Protection du système** > Vérification automatique des fichiers de démarrage
- **Protection en temps réel** > Protection en temps réel du système de fichiers
- **Analyse de l'ordinateur** > Analyse de l'ordinateur à la demande

Les paramètres ThreatSense sont optimisés pour chaque module et leur modification peut avoir une incidence significative sur le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les fichiers exécutables compressés par un compresseur d'exécutables ou pour activer l'heuristique avancée dans la protection en temps réel du système de fichiers, vous pouvez dégrader les performances du système. Il est donc recommandé de ne pas modifier les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module Analyse de l'ordinateur.

4.1.3.1 Objets

La section **Objets** permet de définir les fichiers de l'ordinateur qui vont faire l'objet d'une analyse visant à rechercher les éventuelles infiltrations.

- **Fichiers** : analyse tous les types de fichiers courants (programmes, images, musiques, vidéos, bases de données, etc.).
- **Liens symboliques** : (analyseur à la demande uniquement) analyse un type spécial de fichiers qui contiennent une chaîne de texte interprétée par le système d'exploitation comme chemin d'accès à un autre fichier ou répertoire.
- **Envoyer les fichiers par courrier électronique** : (non disponible dans la protection en temps réel) analyse des fichiers contenant des messages électroniques.
- **Boîtes aux lettres** : (non disponible dans la protection en temps réel) analyse les boîtes aux lettres de l'utilisateur stockées dans le système. L'utilisation inadéquate de cette option peut provoquer des conflits avec votre client de messagerie. Pour en savoir plus sur les avantages et les inconvénients de cette option, reportez-vous à cet article de base de connaissances.
- **Archives** : (non disponible dans la protection en temps réel) analyse les fichiers compressés dans les archives (.rar, .zip, .arj, .tar, etc.).
- **Archives auto-extractibles** : (non disponible dans la protection en temps réel) analyse les fichiers contenus dans des fichiers d'archives auto-extractibles.
- **Fichiers exécutables compressés par un compresseur d'exécutables** : contrairement aux types d'archives standard, les fichiers exécutables compressés par un compresseur d'exécutables sont décompressés en mémoire, en plus des fichiers exécutables compressés statiques standard (UPX, yoda, ASPack, FGS, etc.).

4.1.3.2 Options

Vous pouvez sélectionner dans la section **Options** les méthodes utilisées lors de la recherche d'infiltrations dans le système. Les options suivantes sont disponibles :

- **Base des signatures de virus** : les signatures peuvent détecter et identifier de manière précise et fiable les infiltrations par leur nom à l'aide de la base des signatures de virus.
- **Heuristique** : l'heuristique est un algorithme qui analyse l'activité (malveillante) des programmes. La détection heuristique présente l'avantage de détecter les nouveaux logiciels malveillants qui n'existaient pas auparavant ou qui ne figurent pas dans la liste des virus connus (base des signatures de virus).
- **Heuristique avancée** : cette option utilise un algorithme heuristique unique développé par ESET et optimisé pour la détection de vers informatiques et de chevaux de Troie écrits dans des langages de programmation de haut niveau. L'heuristique avancée améliore de manière significative la capacité de détection du programme.
- **Logiciels publicitaires/Logiciels espions/Logiciels à risque** : cette catégorie comprend les logiciels qui collectent les informations confidentielles sur les utilisateurs sans leur consentement. Elle inclut également les logiciels qui affichent des publicités.

- **Applications potentiellement indésirables** : ces applications ne sont pas nécessairement malveillantes, mais elles peuvent avoir une incidence négative sur les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation de ces applications). Les changements les plus significatifs concernent l'affichage indésirable de fenêtres contextuelles, l'activation et l'exécution de processus cachés, l'utilisation accrue des ressources système, les changements dans les résultats de recherche et les applications communiquant avec des serveurs distants.
- **Applications potentiellement dangereuses** - cette appellation ait référence à des logiciels commerciaux légitimes qui peuvent être mis à profit par des pirates, s'ils ont été installés à l'insu de l'utilisateur. La classification inclut des programmes tels que des outils d'accès à distance. C'est pour cette raison que cette option est désactivée par défaut.

4.1.3.3 Nettoyage

Les paramètres de nettoyage déterminent la façon dont l'analyseur nettoie les fichiers infectés. Trois niveaux de nettoyage sont possibles :

- **Pas de nettoyage** : les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche une fenêtre d'avertissement et permet à l'utilisateur de choisir une action.
- **Nettoyage standard** : le programme essaie de nettoyer ou de supprimer automatiquement tout fichier infecté. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose une sélection d'actions de suivi. Cette sélection s'affiche également si une action prédéfinie ne peut pas être menée à bien.
- **Nettoyage strict** : le programme nettoie ou supprime tous les fichiers infectés (y compris les archives). Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, la fenêtre d'avertissement qui s'affiche propose différentes options.

Avertissement : Dans le mode de nettoyage standard par défaut, le fichier d'archive n'est entièrement supprimé que si tous les fichiers qu'il contient sont infectés. Si l'archive contient également des fichiers légitimes, elle n'est pas supprimée. Si un fichier d'archive infecté est détecté dans le mode Nettoyage strict, le fichier entier est supprimé, même s'il contient également des fichiers intacts.

4.1.3.4 Extensions

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres ThreatSense vous permet de définir les types de fichiers à exclure de l'analyse.

Par défaut, tous les fichiers sont analysés, quelle que soit leur extension. Toutes les extensions peuvent être ajoutées à la liste des fichiers exclus de l'analyse. Les boutons **Ajouter** et **Supprimer** permettent d'activer ou d'empêcher l'analyse des fichiers portant certaines extensions.

L'exclusion de fichiers de l'analyse peut être utile lorsque certains types de fichiers provoquent un fonctionnement incorrect du programme. Par exemple, il peut être judicieux d'exclure les extensions *.log*, *.cfg* et *.tmp*.

4.1.3.5 Limites

La section **Limites** permet de spécifier la taille maximale des objets et les niveaux d'imbrication des archives à analyser :

- **Taille maximale :**définit la taille maximum des objets à analyser. Le module antivirus n'analyse alors que les objets d'une taille inférieure à celle spécifiée. Il n'est pas recommandé de modifier la valeur par défaut et il n'y a généralement aucune raison de le faire. Cette option ne doit être modifiée que par des utilisateurs chevronnés ayant des raisons spécifiques d'exclure de l'analyse des objets plus volumineux.
- **Durée maximale d'analyse :**définit la durée maximum attribuée à l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cesse d'analyser un objet une fois ce temps écoulé, que l'analyse soit terminée ou non.
- **Niveau d'imbrication maximal :**indique la profondeur maximale d'analyse des archives. Il n'est pas recommandé de modifier la valeur par défaut (10). Dans des circonstances normales, il n'y a aucune raison de le faire. Si l'analyse prend fin prématurément en raison du nombre d'archives imbriquées, l'archive reste non vérifiée.
- **Taille de fichiers maximale :**cette option permet de spécifier la taille maximale (après extraction) des fichiers à analyser qui sont contenus dans les archives. Si l'analyse prend fin prématurément en raison de cette limite, l'archive reste non vérifiée.

Si vous souhaitez désactiver l'analyse des dossiers contrôlés par le système (*/proc* et */sys*), sélectionnez l'option **Exclure les dossiers de contrôle système de l'analyse** (cette option n'est pas disponible pour l'analyse au démarrage).

4.1.3.6 Autres

Lorsque l'option Activer l'optimisation intelligente est sélectionnée, les paramètres optimaux sont utilisés de manière à garantir le niveau d'analyse le plus efficace tout en conservant la meilleure vitesse d'analyse. Les différents modules de protection proposent une analyse intelligente en utilisant différentes méthodes et en les appliquant à des types de fichiers spécifiques. L'optimisation intelligente n'est pas définie de manière fixe dans le produit. L'équipe de développement d'ESET Development Team met en œuvre en permanence de nouvelles modifications qui sont ensuite intégrées dans ESET NOD32 Antivirus par l'intermédiaire de mises à jour régulières. Si l'option Activer l'optimisation intelligente est désactivée, seuls les paramètres définis par l'utilisateur dans le noyau ThreatSense de ce module particulier sont appliqués lors de la réalisation d'une analyse.

Analyser l'autre flux de données (analyseur à la demande uniquement)
Les autres flux de données utilisés par le système de fichiers sont des associations de fichiers et de dossiers invisibles pour les techniques ordinaires de détection de virus. De nombreuses infiltrations tentent d'éviter la détection en se

faisant passer pour d'autres flux de données.

Conserver la date et l'heure du dernier accès (analyseur à la demande uniquement)
Cochez cette case pour conserver l'heure d'accès d'origine des fichiers analysés au lieu de la mettre à jour (par exemple, pour l'utiliser avec des systèmes de sauvegarde de données).

4.1.4 Une infiltration est détectée

Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, disquettes, etc.).

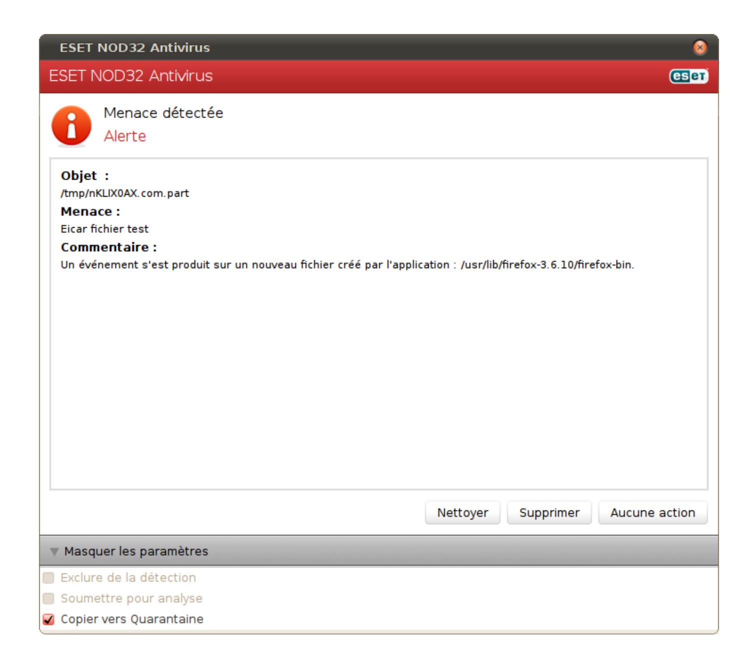
Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, etc.), nous recommandons d'effectuer les opérations suivantes :

1. Ouvrez ESET NOD32 Antivirus et cliquez sur **Analyse de l'ordinateur**.
2. Cliquez sur **Analyse intelligente** (pour plus d'informations, reportez-vous à la section Analyse intelligente 11).
3. Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez des cibles à analyser.

Pour donner un exemple général de la façon dont les infiltrations sont traitées dans ESET NOD32 Antivirus, supposons qu'une infiltration soit détectée par la protection en temps réel du système de fichiers, qui utilise le niveau de nettoyage par défaut. Le programme tente de nettoyer ou de supprimer le fichier. Si aucune action n'est prédéfinie pour le module de protection en temps réel, vous êtes invité à sélectionner une option dans une fenêtre d'avertissement. Généralement, les options **Nettoyer**, **Supprimer** et **Aucune action** sont disponibles. Il n'est pas recommandé de sélectionner **Aucune action**, car les fichiers infectés seraient conservés tels quels. La seule exception concerne les situations où vous êtes sûr que le fichier est inoffensif et a été détecté par erreur.

Nettoyage et suppression : utilisez le nettoyage si un fichier a été attaqué par un virus qui y a joint du code malveillant. Dans ce cas, essayez d'abord de nettoyer le fichier infecté pour le restaurer dans son état d'origine. Si le fichier se compose uniquement de code malveillant, il sera supprimé.



Suppression de fichiers dans des archives : en mode de nettoyage par défaut, l'archive complète n'est supprimée que si elle ne contient que des fichiers infectés et aucun fichier sain. Autrement dit, les archives ne sont pas supprimées si elles contiennent aussi des fichiers sains. Cependant, soyez prudent si vous choisissez un **nettoyage strict** : dans ce mode, l'archive sera supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

4.2 Mise à jour du programme

Des mises à jour régulières d'ESET NOD32 Antivirus sont nécessaires pour conserver le niveau maximum de sécurité. Le module de mise à jour garantit que le programme est toujours à jour en mettant à jour la base de données des signatures de virus.

En cliquant sur **Mettre à jour** dans le menu principal, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire. Pour démarrer manuellement la mise à jour, cliquez sur **Mettre à jour la base des signatures de virus**.

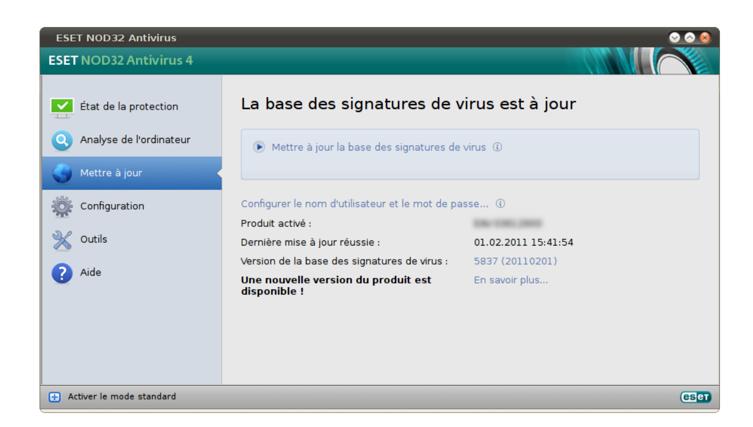
Dans des circonstances normales, lorsque les mises à jour sont téléchargées correctement, le message **La base des signatures de virus est à jour** s'affiche dans la fenêtre Mise à jour. Si la base des signatures de virus ne peut pas être mise à jour, il est recommandé de vérifier les paramètres de mise à jour 15 - la cause la plus courante de cette erreur est une entrée incorrecte de données d'authentification (nom d'utilisateur et mot de passe) ou une configuration incorrecte des paramètres de connexion 21.

La fenêtre Mise à jour contient également la version de la base des signatures de virus. Cette indication numérique est un lien actif vers le site Web d'ESET, qui répertorie toutes les signatures ajoutées dans cette mise à jour.

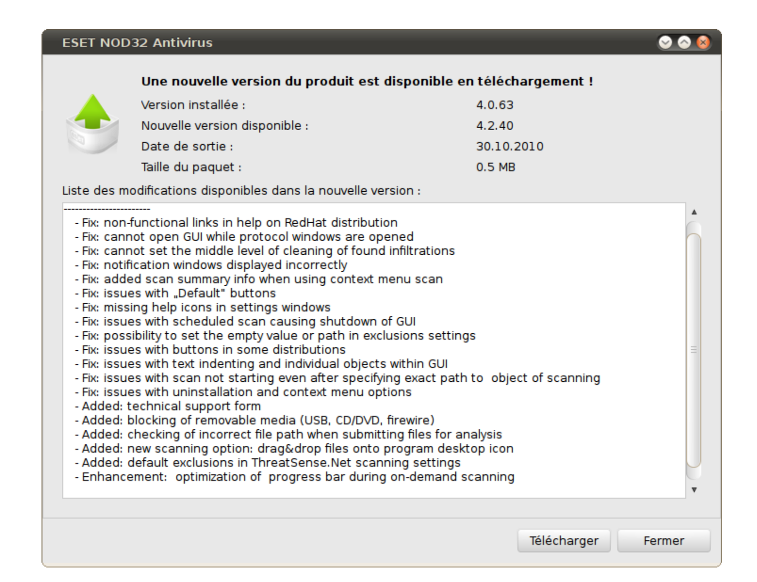
REMARQUE : Votre nom d'utilisateur et votre mot de passe sont fournis par ESET après l'achat d'ESET NOD32 Antivirus.

4.2.1 Mise à niveau vers une nouvelle version

Pour bénéficier d'une protection maximale, il est important d'utiliser la dernière version d'ESET NOD32 Antivirus. Pour vérifier si une nouvelle version est disponible, cliquez sur **Mettre à jour** dans le menu principal situé à gauche. Si une nouvelle version est disponible, le message *Une nouvelle version du produit est disponible !* apparaît au bas de la fenêtre. Cliquez sur **En savoir plus** pour afficher une nouvelle fenêtre contenant le numéro de la nouvelle version et la liste des modifications.



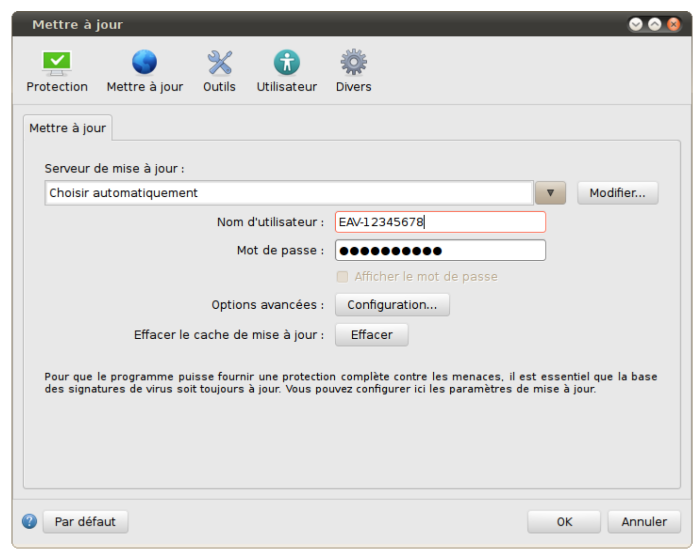
Cliquez sur **Télécharger** pour télécharger la dernière version. Cliquez sur **Fermer** pour fermer la fenêtre et télécharger la mise à niveau ultérieurement.



Si vous avez cliqué sur **Télécharger**, le fichier est téléchargé dans le dossier des téléchargements (ou dans le dossier par défaut défini par votre navigateur). Lorsque le téléchargement du fichier est terminé, lancez le fichier et suivez les instructions d'installation. Votre nom d'utilisateur et votre mot de passe sont transférés automatiquement vers la nouvelle installation. Il est recommandé de vérifier régulièrement si des mises à niveau sont disponibles, en particulier si vous installez ESET NOD32 Antivirus depuis un CD/DVD.

4.2.2 Configuration des mises à jour

La section de la configuration des mises à jour permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour et les données d'authentification donnant accès à ces serveurs. Par défaut, le menu déroulant **Serveur de mise à jour** est défini sur l'option **Choisir automatiquement**, ce qui garantit que les fichiers de mise à jour sont téléchargés automatiquement depuis le serveur ESET en utilisant le moins de ressources réseau possible.



La liste des serveurs de mise à jour disponibles est accessible par l'intermédiaire du menu déroulant **Serveur de mise à jour**. Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier** Saisissez ensuite l'adresse du nouveau serveur dans le champ de saisie **Serveur de mise à jour** et cliquez sur le bouton **Ajouter**. L'authentification des serveurs de mise à jour est basée sur le **nom d'utilisateur** et le **mot de passe** générés et qui vous ont été envoyés après l'achat.

Pour activer l'utilisation du mode test (téléchargement des mises à jour des versions précommerciales), cliquez sur le bouton **Configuration** situé à côté de l'option **Options avancées** et cochez ensuite la case **Activer le mode test**. Pour désactiver l'affichage des notifications dans la partie système de la barre d'état après chaque mise à jour, cochez la case **Ne pas afficher de notification de réussite de la mise à jour**.

Pour supprimer toutes les données de mise à jour stockées temporairement, cliquez sur le bouton **Effacer** situé à côté de l'option **Effacer le cache de mise à jour**. Utilisez cette option si vous rencontrez des problèmes de mise à jour.

4.2.3 Comment créer des tâches de mise à jour

Vous pouvez déclencher les mises à jour manuellement en cliquant sur **Mettre à jour la base des signatures de virus** dans la fenêtre principale qui s'affiche lorsque vous cliquez sur **Mettre à jour** dans le menu principal.

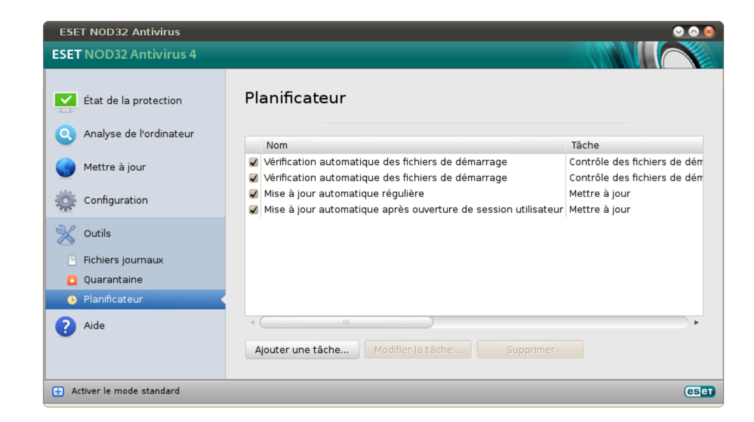
Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET NOD32 Antivirus :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après ouverture de session utilisateur**

Chacune de ces tâches de mise à jour peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez en créer des nouvelles avec vos propres paramètres. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à la section Planificateur 16.

4.3 Planificateur

Le **planificateur** est disponible si l'option Mode avancé dans ESET NOD32 Antivirus est activée. Le Planificateur est accessible depuis le menu principal de ESET NOD32 Antivirus, dans **Outils**. Le **planificateur** contient la liste de toutes les tâches planifiées et des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.



Par défaut, les tâches planifiées suivantes sont affichées dans le planificateur :

- Mise à jour automatique régulière
- Mise à jour automatique après ouverture de session utilisateur
- vérification automatique des fichiers de démarrage ;
- vérification automatique des fichiers de démarrage après la mise à jour réussie de la base des signatures de virus ;
- maintenance des journaux (une fois que l'option **Afficher les tâches système** est activée dans la configuration du planificateur).

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), cliquez avec le bouton droit sur la tâche et cliquez sur **Modifier**. Vous pouvez également sélectionner la tâche à modifier et cliquer sur le bouton **Modifier**.

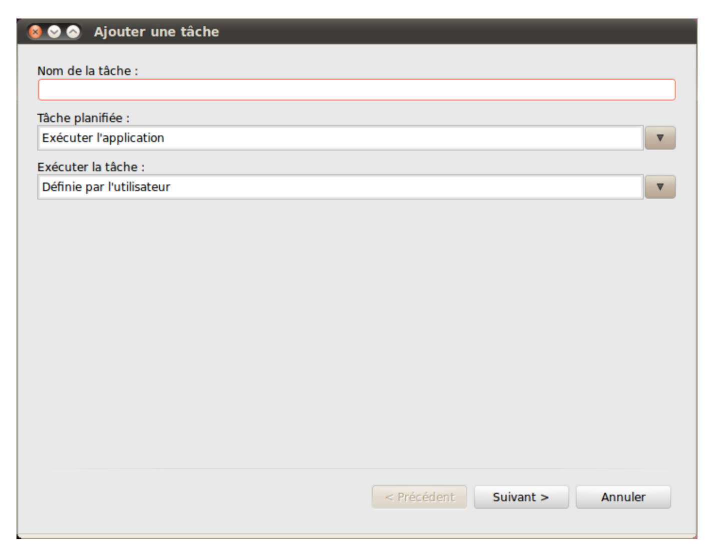
4.3.1 Pourquoi planifier des tâches ?

Le planificateur gère et lance les tâches planifiées qui ont été préalablement définies et configurées. La configuration et les propriétés comprennent des informations telles que la date et l'heure, ainsi que des profils spécifiques à utiliser pendant l'exécution de ces tâches.

4.3.2 Création de nouvelles tâches

Pour créer une nouvelle tâche dans le planificateur, cliquez sur le bouton **Ajouter une tâche...** ou cliquez avec le bouton droit sur la tâche et sélectionnez **Ajouter...** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter l'application**
- **Mettre à jour**
- **Maintenance des journaux**
- **Analyse de l'ordinateur à la demande**
- **Contrôle des fichiers de démarrage du système**



La tâche planifiée la plus fréquente étant la mise à jour, nous allons expliquer comment ajouter une nouvelle tâche de mise à jour.

Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mettre à jour**. Saisissez le nom de la tâche dans le champ **Nom de la tâche**. Sélectionnez la fréquence de la tâche dans le menu déroulant **Exécuter la tâche**. Les options suivantes sont disponibles : **Défini par l'utilisateur**, **Une fois**, **Plusieurs fois**, **Quotidiennement**, **Hebdo** et **Déclenchée par un événement**. Selon la fréquence sélectionnée, vous serez invité à choisir différents paramètres de mise à jour. Vous pouvez définir ensuite l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les trois options suivantes sont disponibles :

- **Patienter jusqu'à la prochaine heure planifiée**
- **Exécuter la tâche dès que possible**
- **Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution dépasse l'intervalle spécifié** (l'intervalle peut être défini à l'aide de la zone de liste déroulante **Intervalle minimal entre deux tâches**)

Dans l'étape suivante, une fenêtre récapitulative apparaît ; elle affiche des informations sur la tâche planifiée en cours. Cliquez sur le bouton **Terminer**.

La nouvelle tâche planifiée sera ajoutée à la liste des tâches planifiées.

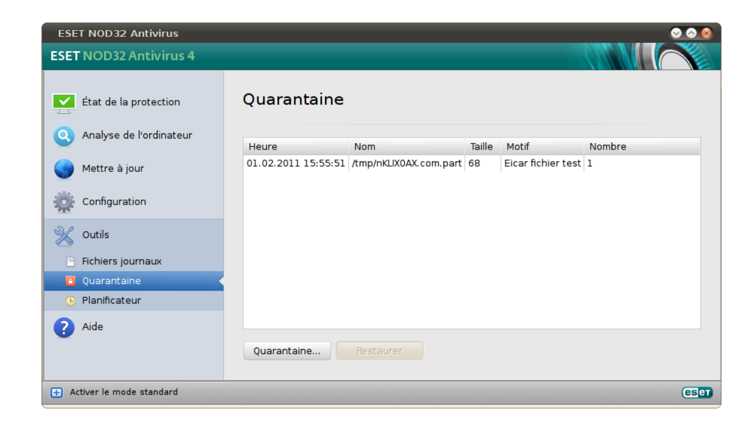
Par défaut, le système contient les tâches planifiées essentielles qui garantissent le fonctionnement correct du produit. Ces tâches ne doivent pas être modifiées et sont

masquées par défaut. Pour modifier cette option et afficher ces tâches, sélectionnez **Configuration** > **Saisie des préférences de l'application...** > **Outils** > **Planificateur** et sélectionnez l'option **Afficher les tâches système**.

4.4 Quarantaine

La principale fonction de la quarantaine est le stockage en toute sécurité des fichiers infectés. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET NOD32 Antivirus.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte mais n'a pas été détecté par l'analyseur antivirus. Les fichiers de la quarantaine peuvent être soumis pour analyse au laboratoire de recherche sur les menaces d'ESET.



Les fichiers du dossier de quarantaine peuvent être visualisés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin de l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (par exemple « ajouté par l'utilisateur ») et le nombre de menaces (par exemple s'il s'agit d'une archive contenant plusieurs infiltrations). Le dossier de quarantaine contenant les fichiers mis en quarantaine (*/var/opt/eset/esets/cache/quarantine*) reste dans le système même après la désinstallation d'ESET NOD32 Antivirus. Les fichiers en quarantaine sont stockés en toute sécurité dans un format crypté et peuvent être restaurés après l'installation d'ESET NOD32 Antivirus.

Si vous souhaitez analyser automatiquement les fichiers en quarantaine après chaque mise à jour de la base des signatures de virus, sélectionnez l'option **Analyser à nouveau les fichiers en quarantaine après chaque mise à jour** dans **Configuration** > **Saisie des préférences de l'application...** > **Outils** > **Quarantaine**.

4.4.1 Mise en quarantaine de fichiers

ESET NOD32 Antivirus déplace automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas annulé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine**. Il est également possible d'utiliser le menu contextuel : cliquez avec le bouton droit dans la fenêtre **Quarantaine**, choisissez le fichier à mettre en quarantaine et cliquez sur le bouton **Ouvrir**.

4.4.2 Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. Utilisez le bouton **Restaurer** ; ce bouton est également accessible depuis le menu contextuel : cliquez avec le bouton droit sur le fichier dans la fenêtre **Quarantaine**, puis cliquez sur **Restaurer**. Le menu contextuel offre également l'option **Restaurer vers...** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

4.4.3 Soumission de fichiers de quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré infecté par erreur (ex. par l'analyse heuristique du code) et placé en quarantaine, envoyez ce fichier au laboratoire de recherche sur les menaces d'ESET. Pour soumettre un fichier de la quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre le fichier pour analyse** dans le menu contextuel.

4.5 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La consignation représente un puissant outil pour l'analyse système, la détection de menaces et le dépannage. La consignation est toujours active en arrière-plan sans interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres de détail actifs. Il est possible de consulter les messages texte et les journaux directement à partir de l'environnement ESET NOD32 Antivirus, ainsi que d'archiver les journaux.

Vous pouvez accéder aux fichiers journaux depuis le menu principal ESET NOD32 Antivirus en cliquant sur **Outils** > **Fichiers journaux**. Sélectionnez le type de journal souhaité dans le menu déroulant **Journal**, en haut de la fenêtre. Les journaux suivants sont disponibles :

1. **Menaces détectées** : cette option permet de consulter toutes les informations concernant les événements liés à la détection d'infiltrations.
2. **Événements** : cette option permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Toutes les actions importantes exécutées par ESET NOD32 Antivirus sont enregistrées dans les journaux des événements.
3. **Analyse de l'ordinateur** : cette fenêtre affiche toutes les analyses effectuées. Double-cliquez sur une entrée pour afficher les détails de l'analyse de l'ordinateur à la demande correspondante.

Vous pouvez copier les informations affichées dans chaque section directement dans le Presse-papiers en sélectionnant l'entrée souhaitée, puis en cliquant sur le bouton **Copier**.

4.5.1 Maintenance des journaux

La configuration de la consignation d'ESET NOD32 Antivirus est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration** > **Saisie des préférences de l'application...** > **Outils** > **Fichiers journaux**. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

- **Supprimer les anciennes entrées du journal automatiquement** : les entrées de journal plus anciennes que le nombre de jours spécifié sont automatiquement supprimées.
- **Optimiser automatiquement les fichiers journaux** : permet la défragmentation des fichiers journaux si le pourcentage spécifié d'enregistrements inutilisés est dépassé.

Pour configurer l'option **Filtre par défaut des entrées du journal**, cliquez sur le bouton **Modifier** et sélectionnez/désélectionnez les types de journaux en fonction de vos besoins.

4.5.2 Filtrage des journaux

Les journaux stockent des informations sur les événements système importants : La fonctionnalité de filtrage des journaux permet d'afficher des entrées concernant un type d'événement spécifique.

Les types de journaux les plus fréquents sont répertoriés ci-dessous :

- **Avertissements critiques** : erreurs système critiques (par exemple, le démarrage de la protection antivirus a échoué).
- **Erreurs** : messages d'erreur du type *Erreur de téléchargement de fichier* et erreurs critiques.
- **Avertissements** : messages d'avertissement.
- **Entrées informatives** : messages d'informations concernant des mises à jour réussies, des alertes, etc.
- **Entrées de diagnostic** : informations nécessaires au réglage du programme et de toutes les entrées décrites ci-dessus.
- **Tous les filtres** : cochez cette case pour sélectionner/désélectionner tous les types de journaux ci-dessus.

4.6 Interface utilisateur

La configuration de l'interface utilisateur d'ESET NOD32 Antivirus peut être modifiée de manière à pouvoir ajuster l'environnement de travail selon vos besoins. Ces options de configuration sont accessibles depuis la section **Configuration** > **Saisie des préférences de l'application...** > **Utilisateur** > **Interface**.

Dans cette section, l'option de mode avancé permet aux utilisateurs de passer au mode avancé. Le mode avancé affiche des paramètres détaillés et des commandes supplémentaires pour ESET NOD32 Antivirus.

Pour activer l'écran d'accueil, sélectionnez l'option **Afficher l'écran de démarrage**.

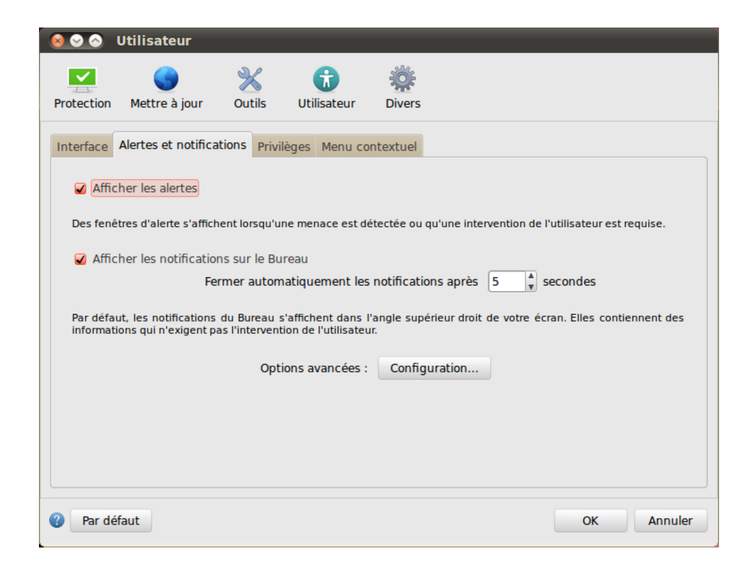
Dans la section **Utiliser le menu standard**, vous pouvez sélectionner les options **En mode standard**/**En mode avancé** afin d'autoriser l'utilisation du menu standard dans la fenêtre principale du programme dans l'affichage correspondant.

Pour activer l'utilisation des info-bulles, sélectionnez l'option **Afficher les info-bulles**. L'option **Afficher les fichiers masqués** vous permet d'afficher et de sélectionner les fichiers cachés dans la configuration des **cibles à analyser** dans une **analyse de l'ordinateur**.

4.6.1 Alertes et notifications

La section **Alertes et notifications** vous permet de configurer le mode de traitement des alertes en cas de menace et des notifications système dans ESET NOD32 Antivirus.

La désactivation de l'option **Afficher les alertes** annule les fenêtres d'alerte et n'est adaptée qu'à des situations très précises. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée).



La sélection de l'option **Afficher les notifications sur le Bureau** active l'affichage des fenêtres d'alerte sur le bureau (par défaut dans l'angle supérieur droit de votre écran) sans aucune intervention de l'utilisateur. Vous pouvez définir la période pour laquelle une notification est affichée en réglant la valeur **Fermer automatiquement les notifications après** X **secondes**.

4.6.1.1 Configuration avancée des alertes et notifications

Afficher uniquement les notifications nécessitant une interaction de l'utilisateur
Avec cette option, vous pouvez activer l'affichage des messages qui nécessitent l'intervention de l'utilisateur.

Afficher uniquement les notifications exigeant une intervention de l'utilisateur lors de l'exécution d'applications en mode plein écran
Cette option est utile lorsque vous utilisez des présentations, jouez à des jeux ou toute autre activité nécessitant l'intégralité de l'écran.

4.6.2 Privilèges

Les paramètres ESET NOD32 Antivirus peuvent être très importants pour la stratégie de sécurité de votre organisation. Des modifications non autorisées peuvent mettre en danger la stabilité et la protection de votre système. Par conséquent, vous pouvez choisir les utilisateurs qui sont autorisés à modifier la configuration du programme.

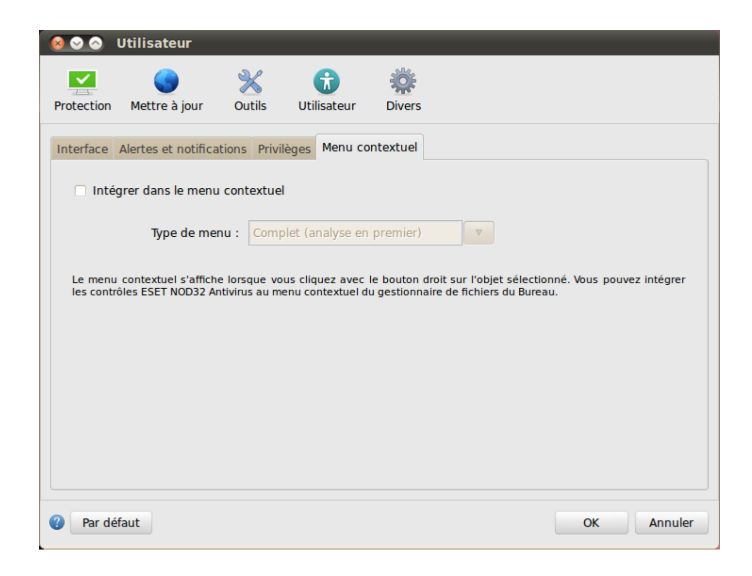
Pour définir les utilisateurs privilégiés, accédez à **Configuration** > **Saisie des préférences de l'application...** > **Utilisateur** > **Privilèges**.

Il est essentiel que le programme soit correctement configuré pour garantir le maximum de sécurité au système. Tout changement non autorisé peut faire perdre des données importantes. Pour définir la liste des utilisateurs privilégiés, il vous suffit de sélectionner les utilisateurs dans la liste **Utilisateurs** dans la partie gauche et cliquez sur le bouton **Ajouter**. Pour supprimer un utilisateur, sélectionnez son nom dans la liste **Utilisateurs privilégiés** située à droite, puis cliquez sur **Supprimer**.

REMARQUE : Si la liste des utilisateurs privilégiés est vide, tous les utilisateurs du système sont autorisés à modifier les paramètres du programme.

4.6.3 Menu contextuel

L'intégration des menus contextuels peut être activée dans la section **Configuration** > **Saisie des préférences de l'application...** > **Utilisateur** > **Menu contextuel** en activant la case à cocher **Intégrer dans le menu contextuel**.



REMARQUE : pour activer l'intégration des menus contextuels, vérifiez que l'extension nautilius-actions est installée.

4.7 ThreatSense.Net

Le système d'alerte anticipé ThreatSense.Net est un outil qui permet d'informer ESET immédiatement et en permanence de l'existence de nouvelles infiltrations. Le système d'alerte anticipé bidirectionnel ThreatSense.Net n'a qu'un seul objectif : améliorer la protection que nous vous offrons. Le meilleur moyen de voir les nouvelles menaces dès qu'elles apparaissent est d'être en contact permanent avec le plus grand nombre de nos clients et de les utiliser comme des « éclaireurs ». Deux options sont possibles :

1. Vous pouvez décider de ne pas activer le système d'alerte anticipé ThreatSense.Net. Vous ne perdez rien de la fonctionnalité du logiciel et vous bénéficiez toujours la meilleure protection que nous offrons.
2. Vous pouvez configurer le système d'alerte anticipé ThreatSense.Net afin d'envoyer des informations anonymes qui concernent les nouvelles menaces et indiquent l'endroit où se trouve le code menaçant. Ce fichier peut être envoyé à ESET pour une analyse détaillée. En étudiant ces menaces, ESET met à jour sa base de données des menaces et améliore ses capacités à détecter les menaces dans le programme.

Le système d'alerte anticipé ThreatSense.Net collecte sur votre ordinateur des informations concernant les nouvelles menaces détectées. Ces informations comprennent un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin et le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Bien qu'il y ait une probabilité de divulgation au laboratoire de recherche sur les menaces d'ESET de certaines informations vous concernant ou concernant votre ordinateur (noms d'utilisateur dans un chemin de répertoire), ces informations ne seront utilisées à AUCUNE autre fin que pour répondre immédiatement aux nouvelles menaces.

La configuration de ThreatSense.Net est accessible depuis la fenêtre Configuration avancée, dans **Outils** > **ThreatSense.Net** . Sélectionnez l'option **Activer le système d'alerte anticipée ThreatSense.Net** pour activer le système, puis cliquez sur le bouton **Configuration** situé à côté de l'en-tête Options avancées.

4.7.1 Fichiers suspects

L'onglet Fichiers suspects permet de configurer la manière dont les menaces sont soumises pour analyse au laboratoire de recherche sur les menaces d'ESET.

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire de recherche sur les menaces pour analyse. S'il s'avère d'une application malveillante, sa détection sera ajoutée à la prochaine mise à jour de la base des signatures de virus.

Soumission des fichiers suspects : vous pouvez choisir d'envoyer ces fichiers **Pendant la mise à jour** : ils seront soumis au laboratoire de recherche sur les menaces d'ESET

pendant une mise à jour régulière de la base des signatures de virus. Vous pouvez également choisir de les envoyer **Dès que possible** : ce paramètre convient si une connexion Internet permanente est disponible.

Si vous ne souhaitez pas soumettre de fichiers, sélectionnez l'option **Ne pas soumettre**. Le fait de choisir de ne pas soumettre les fichiers à analyse n'a pas d'incidence sur la soumission des informations statistiques qui est configurée dans un autre secteur.

Le système d'alerte anticipé ThreatSense.Net collecte sur votre ordinateur des informations anonymes concernant les nouvelles menaces détectées. Ces informations peuvent inclure le nom de l'infiltration, la date et l'heure de détection, la version du produit de sécurité ESET, ainsi que des informations sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Les statistiques sont normalement fournies aux serveurs ESET une ou deux fois par jour.

Voici un exemple d'informations statistiques envoyées :

```
# utc_time=2009-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=2.6.18-128.e5
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=/home/user/Documents/Incoming/rdgFR1463
[1].zip
```

Soumission des informations statistiques anonymes : vous pouvez définir le moment de l'envoi des informations statistiques. Si vous choisissez d'envoyer les informations statistiques **Dès que possible**, elles sont envoyées immédiatement après leur création. Ce choix convient si une connexion Internet est disponible en permanence. Si l'option **Pendant la mise à jour** est sélectionnée, toutes les informations statistiques sont envoyées pendant la mise à jour qui suit leur collecte.

Si vous ne souhaitez pas envoyer d'informations statistiques, vous pouvez sélectionner l'option **Ne pas soumettre**.

Filtre d'exclusion : cette option permet d'exclure certains fichiers/dossiers de la soumission. Par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, tels que des documents ou des feuilles de calcul. Les fichiers les plus ordinaires sont exclus par défaut (*.doc*, etc.). Vous pouvez ajouter des types de fichiers à la liste des fichiers exclus.

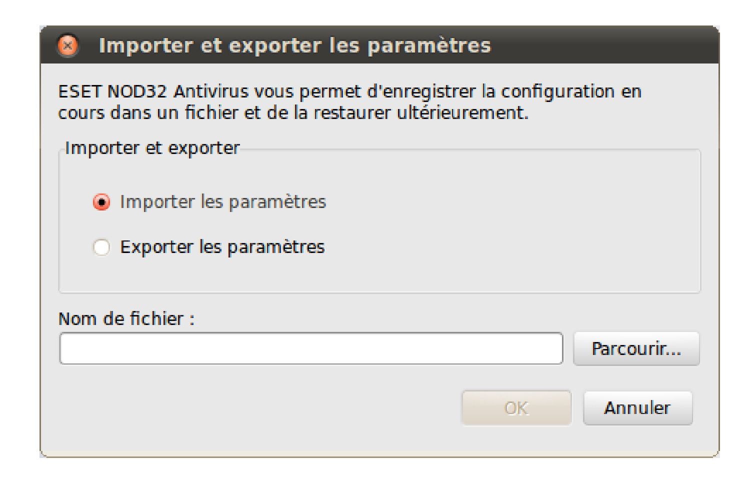
Adresse électronique de contact : votre adresse électronique peut être envoyée avec les fichiers suspects et peut être utilisée pour vous contacter si des informations complémentaires sont nécessaires pour l'analyse. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires s'avèrent nécessaires.

5. Utilisateur chevronné

5.1 Importer et exporter les paramètres

L'importation et l'exportation des configurations d'ESET NOD32 Antivirus sont disponibles en Mode avancé dans **Configuration**.

Les opérations d'importation et d'exportation utilisent des fichiers d'archive pour stocker la configuration. Ces opérations sont utiles si vous devez sauvegarder la configuration actuelle d'ESET NOD32 Antivirus pour l'utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration ESET NOD32 Antivirus préférée sur plusieurs systèmes. Il leur suffit d'importer le fichier de configuration pour transférer les paramètres souhaités.



5.1.1 Importer les paramètres

L'importation d'une configuration est très facile. Dans le menu principal, cliquez sur **Configuration** > **Importer et exporter les paramètres...**, puis sélectionnez l'option **Importer les paramètres**. Saisissez le nom du fichier de configuration ou cliquez sur le bouton **Parcourir...** pour accéder au fichier de configuration à importer.

5.1.2 Exporter les paramètres

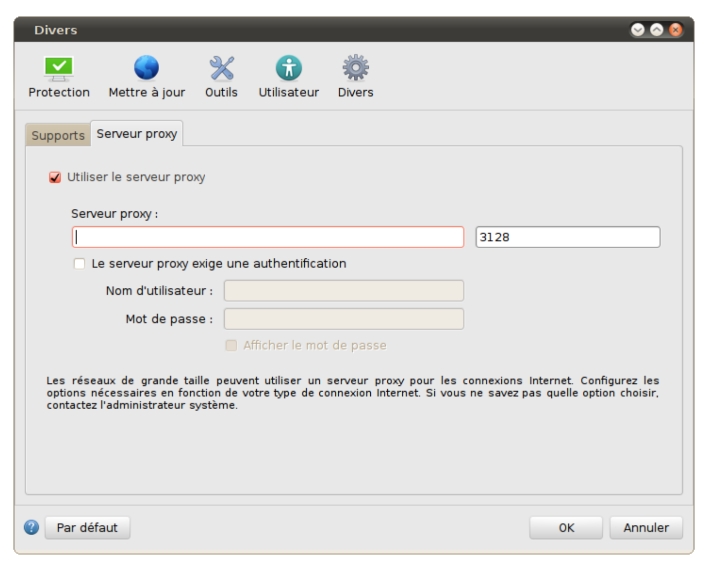
La procédure d'exportation d'une configuration est très semblable. Dans le menu principal, cliquez sur **Configuration** > **Importer et exporter les paramètres...**. Sélectionnez l'option **Exporter les paramètres** et entrez le nom du fichier de configuration. Utilisez le navigateur pour sélectionner un emplacement de votre ordinateur pour enregistrer le fichier de configuration.

5.2 Configuration du serveur proxy

Les paramètres de serveur proxy peuvent être configurés dans **Divers** > **Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour l'intégralité d'ESET NOD32 Antivirus. Les paramètres définis ici seront utilisés par tous les modules exigeant une connexion à Internet.

Pour spécifier des paramètres de serveur proxy à ce niveau, cochez la case **Utiliser un serveur proxy**, puis entrez l'adresse du serveur proxy dans le champ **Serveur proxy**, ainsi que le numéro de port de ce serveur proxy.

Si la communication avec le serveur proxy exige une authentification, cochez la case **Le serveur proxy nécessite une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants.



5.3 Blocage de supports amovibles

Les supports amovibles (CD ou clé USB) peuvent contenir du code malveillant et constituer un risque pour votre ordinateur. Pour bloquer les supports amovibles, cochez la case **Activer le blocage des supports amovibles**. Pour autoriser l'accès à certains types de supports, désélectionnez les volumes souhaités.

6. Glossaire

6.1 Types d'infiltrations

Une infiltration est un élément de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur et/ou de l'endommager.

6.1.1 Virus

Un virus est une infiltration qui endommage les fichiers existants de votre ordinateur. Les virus informatiques sont comparables aux virus biologiques parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre.

Les virus informatiques attaquent principalement les fichiers, scripts et documents exécutables. Pour proliférer, un virus attache son « corps » à la fin d'un fichier cible. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution du fichier infecté, le virus s'active lui-même (avant l'application originale) et exécute sa tâche prédéfinie. C'est après seulement que l'application originale peut s'exécuter. Un virus ne peut pas infecter un ordinateur à moins qu'un utilisateur n'exécute ou n'ouvre lui-même le programme malveillant (accidentellement ou délibérément).

Les virus peuvent varier en fonction de leur gravité et de leur cible. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres, en revanche, ne causent pas de réels dommages : ils ne servent qu'à gêner l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Il est important de noter que, contrairement aux chevaux de Troie et aux logiciels espions, les virus sont de plus en plus rares, car d'un point de vue commercial, ils ne sont pas très attrayants pour les auteurs de programmes malveillants. En outre, le terme « virus » est souvent utilisé mal à propos pour couvrir tout type d'infiltrations. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Si votre ordinateur est infecté par un virus, il est nécessaire de restaurer les fichiers infectés à leur état original, c'est-à-dire de les nettoyer à l'aide d'un programme antivirus.

Dans la catégorie des virus, on peut citer : *OneHalf*, *Tenga* et *Yankee Doodle*.

6.1.2 Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence fondamentale entre les virus et les vers est que les vers ont la capacité de se répliquer et de voyager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire d'adresses de messagerie de votre liste de contacts ou exploitent les vulnérabilités de sécurité des applications réseau.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rend plus dangereux que les autres types de programmes malveillants.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. Par nature, il peut servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés, car ils contiennent probablement du code malicieux.

Parmi les vers les plus connus, on peut citer : *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* et *Netsky*.

6.1.3 Chevaux de Troie

Les chevaux de Troie étaient auparavant définis comme une catégorie d'infiltrations dont la particularité est de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter. Aujourd'hui, les chevaux de Troie n'ont plus besoin de se faire déguiser. Leur unique objectif est de trouver la manière la plus facile de s'infiltrer pour accomplir leurs desseins malveillants. Le terme « cheval de Troie » est donc devenu un terme très général qui décrit toute infiltration qui n'entre pas dans une catégorie spécifique.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- Downloader : programme malveillant qui est en mesure de télécharger d'autres infiltrations sur Internet.
- Dropper : type de cheval de Troie conçu pour déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- Backdoor : application qui communique à distance avec les pirates et leur permet d'accéder à un système et d'en prendre le contrôle.
- Keylogger : programme qui enregistre chaque touche sur laquelle tape l'utilisateur et envoie les informations aux pirates.
- Dialer : programme destiné à se connecter à des numéros surtaxés. Il est presque impossible qu'un utilisateur remarque qu'une nouvelle connexion a été créée. Les dialers ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.
- Les chevaux de Troie prennent généralement la forme de fichiers exécutables. Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il contient sans doute du code malveillant.

Parmi les chevaux de Troie les plus connus, on peut citer : *NetBus*, *Trojandownloader.Small.ZL*, *Slapper*.

6.1.4 Logiciels publicitaires

Le terme anglais « adware » désigne les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Les logiciels publicitaires ouvrent généralement une nouvelle fenêtre contextuelle automatiquement dans un navigateur Internet. Cette fenêtre contient de la publicité ou modifie la page de démarrage du navigateur. Ils sont généralement associés à des programmes gratuits et permettent aux développeurs de ces programmes de couvrir les frais de développement de leurs applications (souvent utiles).

Les logiciels publicitaires proprement dits ne sont pas dangereux ; tout au plus dérangent-ils les utilisateurs en affichant ces publicités. Le danger tient dans le fait qu'ils peuvent aussi avoir des fonctions d'espionnage (comme les logiciels espions).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertiront en effet qu'ils installent en plus un programme publicitaire. Souvent, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire.

Certains programmes refuseront de s'installer sans leur logiciel publicitaire ou verront leurs fonctionnalités limitées. Cela signifie que les logiciels publicitaires accèdent souvent au système d'une manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, mieux vaut jouer la sécurité. Si un logiciel publicitaire est détecté sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

6.1.5 Logiciels espions

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Les logiciels espions utilisent des fonctions de traçage pour envoyer diverses données statistiques telles que la liste des sites Web visités, les adresses e-mail de la liste de contacts de l'utilisateur ou la liste des touches du clavier utilisées.

Les auteurs de ces logiciels espions affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne sont pas utilisées à des fins frauduleuses. Les données récupérées par les logiciels espions peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les logiciels espions sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un logiciel espion au cours de l'installation d'un programme qui vise à les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des logiciels espions, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de logiciels espions : ils semblent être des programmes anti-logiciel espion alors qu'ils sont en réalité eux-mêmes des logiciels espions.

Si un fichier est détecté comme étant un logiciel espion sur votre ordinateur, il est recommandé de le supprimer, car il existe une forte probabilité qu'il contienne du code malveillant.

6.1.6 Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. ESET NOD32 Antivirus permet de détecter ces menaces.

Les applications potentiellement dangereuses rentrent dans une classification utilisée pour les logiciels commerciaux légitimes. Cette classification comprend les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur).

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous l'ayez installée), consultez l'administrateur réseau ou supprimez l'application.

6.1.7 Applications potentiellement indésirables

Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres qui n'existaient pas auparavant ;
- activation et exécution de processus cachés ;
- augmentation des ressources système utilisées ;
- modification des résultats de recherche ;
- communication avec des serveurs distants.